724

PRESENTATION 3.2.1

N91-17039

ADVANCE AVIONICS SYSTEM ARCHITECTURES

SPACE TRANSPORTATION AVIONICS SYMPOSIUM
FLIGHT ELEMENTS

ADVANCED AVIONICS SYSTEMS ARCHITECTURES

SCOPE

The idea that an avionics system has, or should have, an architecture is a notion that has come about slowly over the past twenty years. Avionic systems began as individual controllers typically associated with individual vehicle subsystems. As the controllers became based on digital technology, opportunities for information exchange between subsystems increased because digital data bus technology permitted the information to be exchanged without the degradation associated with analog signal transmission. Vehicle subsystems became integrated by sharing information to improve vehicle performance or to avoid the expense and weight of duplicated information sources. The flexibility of digital information sharing provided additional opportunities for changing systems once they were constructed since all that was required in many cases were software changes. The rush to interconnect digital systems has been somewhat of a mixed benefit since system complexity grows as at least a power of the number of connections and perhaps exponentially. Even the accounting task of tracking information sources and users can become formidable. A result has traditionally been that the supposedly "free" information exchange resource becomes choked trying to accommodate the transmission requirements imposed after the system has been constructed. All too often systems are designed using the best engineering judgement and then bludgeoned into submission on the laboratory floor. There is the question of organizational responsibility when subsystems that have been the responsibility of separate organizations become interdependent. For example, it is feasible to use the high-quality rate information from inertial platforms, historically a navigation function, to stabilize the vehicle, a control function with much higher reliability requirement. Which organization controls the platform? There are many such new questions that come about as traditional boundaries between subsystems break down and the vehicle itself becomes the boundary. It is not now feasible to address all questions that can be raised as a result of attempting to design integrated system architectures. An appropriate limitation of the scope of this topic is to consider the avionic flight system as the substrate upon which the applications are built, and as such, must support airborne, and one-time ground functions such as guidance and control, health monitoring, ground maintenance diagnostics, etc. If a sufficiently good understanding of the capabilities and limitations of a useful class of architectures and their requirements can be obtained such that it is feasible to make sound engineering decisions before fabrication, that would be a reasonable and useful goal. The study of digital avionics system architectures is just being accepted as a separate topic. Fault-tolerance is an aspect of systems architecture that, while it may appear to be a cure-all for system failure, has many subtleties that limit its effectiveness. Some important concepts have been identified such as system synchronization and protection against inconsistent data distribution, but a general theoretical framework for system architectures is a future goal.

OBJECTIVES

Space transportation objectives are associated with transporting materiel from Earth to orbit, interplanetary travel and planetary landing. The objectives considered here are associated primarily with Earth to orbit transportation. Many good avionics architectural features will support all phases of space transportation, but interplanetary transportation poses significantly different problems such as long mission times with high-reliability, unattended operation, and significantly different opportunities such as long non-operational flight segments that can be used for equipment fault diagnosis and repair. Although it is not further considered in this write-up, the maintenance of system operation for long mission times is a "hole" in current research since fault-tolerance does no good if the underlying physical devices do not exhibit some minimal reliability for the entire mission. With the trend toward smaller geometries and new physical technologies, it is quite likely that heretofore unimportant failure modes will become dominant over long mission times. Avionic systems that are used in the Earth to orbit scenario can be years in production and months in assembly and checkout on the launch pad. The system life culminates in a ten minute operation with some factors such as acceleration, vibration and temperature dramatically different from anything previously encountered other than during system qualification in the qualification laboratory. The launches tend to be infrequent and very expensive with very expensive payloads. They involve hundreds of launch site personnel servicing a vehicle, using complex scheduling to allow each subsystem expert time in the very limited area around the vehicle. When the vehicle is ready, the launch is subject to the vagaries of the weather and to the pressures of fixed launch windows. Avionics systems for launch vehicles should be designed and fabricated to support worthwhile goals such as low recurring hardware and operations cost, launch on demand, flexible and secure interfaces for payloads and other integrated non-avionics systems, and be open ended to grow and change within the relatively long service life of launch vehicles. Some specific objectives for launch vehicle architectures should be selected to achieve improved reliability at lower cost. Fault-tolerance can be used to permit continued operation with faulty units, not only during launch but also, and perhaps with more impact, during pre-launch activities. Completing subsystem tests without stand-down for avionic systems repair can save facility and personnel time that is much more expensive than the electronics. This will be especially beneficial because, except for the factors noted above, the avionic system operates at rated performance during system checkout, which may take weeks, and may even support factory assembly and health monitoring for months. Ground operations can be stressful in ways different from the launch. For example, ground temperature stress can vary greatly and be sustained for much longer than flight stress. Also, work on other systems can inadvertently stress the avionics and vice versa. Launching the vehicle with faults is problematical since the idea of committing an expensive vehicle to launch with an inexpensive part failed will require a cultural change within the launch vehicle community. If acceptable criteria can be established, vehicle life-cycle costs can be lowered by permitting launch with faults. Another beneficial specific objective is to design avionics subsystems to go from factory to flight without calibration or other adjustments. Suitable internal diagnostics and criteria must be provided to permit satisfactory operation to be confirmed by launch site personnel and to allow ease of fault isolation, change-out and retest in case of failure. As principles of system architecture design become established through research, these should be applied to all avionic systems across the entire vehicle from sensor to effector to provide a uniform basis for measuring avionic system performance through such features as common interfaces and subsystem redundancy management procedures. The specific physical technologies may be different for different functions, for example the engine controller may require high temperature electronics, but the underlying elements for functions such as synchronization and redundancy management could be uniform over the entire avionic system. Diagnostic routines and architecture modeling would then provide detailed insight into avionic system health. Since the avionic systems are becoming more capable and are not the time or cost drivers for checkout, they will have to aid the diagnostics and integration for other subsystems. An important objective in this case will be to establish the avionic system capability to accommodate perhaps thousands of measurements and hundreds of control functions. This implies a large quantity of data, even if individual measurement is taken at a low data rate. On-demand subsystem health data has been suggested as a means to gather data from subsystems when significant changes occur, thus reducing the background data rate to a low level. This approach may be beneficial when subsystem events occur at random, but a global event such as a lightning upset could cause many subsystems to try to report the event simultaneously causing data overload.

SIGNIFICANT RESEARCH ACTIVITIES

The most significant recent research activity targeted at launch vehicle avionics has been the Advanced Launch System (ALS) Advanced Development program. The Advanced Launch System is conceived to be a series of medium to large launch vehicles with the common characteristic that the cost of placing a pound of payload in orbit will be roughly an order of magnitude less than the Titan IV reference-mission cost. In order to meet this goal, it is proposed to utilize advanced, fault-tolerant avionics to support concepts such as knowledge-based system diagnostics for autonomous pre-launch checkout and advanced guidance and control to permit launches in a wider variety of weather conditions than are now possible. The ALS program has, under the title of Multi-path Redundant Avionic Systems (MPRAS) leveraged on-going research efforts at both NASA and Air Force laboratories to develop the required launch vehicle systems. One such effort is being conducted at The Charles Stark Draper Laboratory (CSDL) as the NASA-sponsored Advanced Information Processing System (AIPS). The AIPS program is developing technology that will apply to a wide variety of system needs. It embodies the latest concepts for achieving fault tolerance, graded to be appropriate to the individual function being performed and is designed to be validated to the required reliability and performance. The AIPS concept is illustrated in figure 1 and embodies the advanced architectural concepts that will be covered in the section on technology issues. Another MPRAS effort is being conducted at Boeing Aerospace and is leveraging the Integrated Fault-Tolerant Avionic System (IFTAS, figure 2) to provide capabilities similar to those of the AIPS. A third MPRAS effort is underway at General Dynamics Space Systems, leveraged from Air Force Pave Pillar avionics concepts as illustrated in figure 3. Martin Marietta is developing a large laboratory with a focus on developing reliable, fault-tolerant systems for launch vehicles. The Space Station Freedom data management system architecture illustrated in figure 4 shows a point design with many fault-tolerance features. A significant source of fault-tolerant avionics experience can be found in aircraft systems. Aircraft systems have not labored under the extreme weight sensitivity and reluctance to technological change of most launch vehicle avionics systems (Shuttle is one exception), so that redundancy has for many years been an accepted way to accommodate aircraft system faults. Both in civilian and military aircraft systems, redundant, fault-tolerant avionics have been successfully used in the operational environment of scheduled arrivals and departures to which the space transportation community aspires. The consequences of aircraft avionics system failure are typically not catastrophic, although both commercial and military systems are close to being used for full-time, flight-critical functions where system failure would have the same catastrophic impact as a launch vehicle system failure. All of the major U.S. airframe manufacturers have, in partnership with avionics manufacturers, fielded fault-tolerant avionic systems for high reliability applications, most notably for autoland where the autoland function is critical for up to a minute of flight just prior to touchdown. Fault-tolerance for single function applications appears reasonably well accepted, but the aircraft systems designers are still wrestling with the problem of designing vehicle-wide avionic systems that are manageable and exhibit sufficiently long time between maintenance. Advanced vehicle-wide architectures for military applications are being pursued at Wright Research and Development Center under the Pave Pillar and Pave Pace programs which feature very high performance architectural elements to support various fault tolerance strategies and which are being rendered into hardware using a common module approach to promote lower production and maintenance costs. Honeywell has for a number of years been developing the concept of self-checking pairs to achieve high fault detection coverage for processors, buses and the checkers themselves. This concept is illustrated in figure 5. Self checking pairs is one of the main features MPRAS has defined to enhance Pave Pillar designs. There has been recently renewed interest in protection of avionic hardware from electromagnetic disturbances from natural causes such as lightning or man made high energy radio frequency emissions. This aspect of avionic system design is being most visibly pursued by Honeywell although it is a recognized problem within the aerospace industry. Launch vehicle launch-on-demand capabilities are somewhat dependent on lightning hardness to minimize the need to avoid lightning strikes during ascent. Transients from other, less well defined sources can cause faults in the form of single event upsets that, although they cause no permanent damage, can alter the performance of avionic systems in harmful ways. In addition to these efforts many universities have significant results that can be incorporated into the design and testing of fault-tolerant avionic systems. Table 1 is a list of organizations known to have significant efforts in fault tolerant avionic systems. Most aerospace companies now have more than a passing interest in fault tolerant systems since their use has become pervasive in flight vehicles. Table 2 lists some of the more prominent periodical publications and conferences where technical discussions of advanced avionics are to be found.

TECHNOLOGY ISSUES

Avionic system architecture impacts and is impacted by virtually everything within the vehicle since the digital systems are increasingly used to integrate the activities of vehicle subsystems to achieve performance unattainable with more traditional engineering approaches. The capability of digital avionics, with logic unfettered by the laws of physics, to direct otherwise mundane systems to perform brilliantly in concert is a powerful reason to employ such systems. Unfortunately, the same logic that can correctly find the few ways to make things go right can also make things go wrong in an almost infinite number of ways. The unimaginable complexity of digital systems cannot in general be managed by appeals to physical properties since they are designed out of practical consideration by the nature of the digital logic. Correct design of digital systems is a technology issue that becomes increasingly difficult to manage with the trend toward distributed, fault-tolerant systems. Since most fault-tolerant architectures use replicated, identical elements to protect against random physical failures, a design flaw becomes a generic failure for the entire system. The systems can be modeled as an aid to understanding but testing alone cannot be used for system validation because of the large state spaces that must be tested. Fault-tolerance brings with it the possibility of reducing the failure probability of avionics systems to a negligible amount. However, once the more prominent failure modes have been covered using fault-tolerance, other failure modes become important and they are generally much more subtle and hard to identify, much less quantify. The reliability of the fault-tolerant system becomes almost totally dependent on the fault-tolerance mechanism. This is especially true of reconfigurable fault-tolerant systems since the reconfiguration mechanism can disable good units in response to unexpected inputs or its own internal faults. Therefore, design correctness and a comprehensive accounting of all possible inputs and actions are of paramount importance.

As the digital processing and bus capability keep expanding, and volume per MIPS shrinks, the feasibility and benefit of more integrated non-avionic systems has also increased. The mix of computation and input/output is changing such that I/O accounts for an estimated 75 percent of the avionic system and an even greater portion of system unreliability and cost, because the I/O must service a variety of subsystems and cannot be made as uniform and modular as the computation system. The technology to support effective and efficient input/output design and validation is a new and different area for the avionic systems technologist.

Software development for avionics systems is a critical issue because of the special need for correctness of the system software. There is much less opportunity to check the correctness of system software because the totally logical aspects of digital systems typically have fewer independent correctness criteria to check against. There is also less time to do checking because the system software must be executed more often than application software. Software development environments and languages must be tailored to support system as well as application development. Architectures that are based on combinations of a small number of well understood building blocks offer a means to limit complexity, but the utility of such approaches has yet to be demonstrated. Space systems traditionally use single string systems with individual components qualified to the highest levels. Whether a less costly system of higher reliability can be assembled using lower reliability parts is an issue currently under examination both from technological and cultural standpoints. Aircraft systems used in commercial or military operational situations can be dispatched with a given number of faults, and this is a key to practical systems utilization since it is exceedingly difficult to achieve a perfect operational state, especially where the systems must be serviced and maintained by personnel who are not experts dedicated to particular hardware items. Hardening avionic systems against external electromagnetic disturbances and random transients is a difficult problem since the electromagnetic threats and random transients have not been completely characterized for all threat sources. The effects of transients and electromagnetic disturbances on digital systems are difficult to characterize since they are less well contained than the isolated one-at-a-time faults that traditional fault-tolerance schemes protect against.

SUMMARY

Avionics systems are entering a phase of development where the traditional approaches to satisfactory systems based on engineering judgement and thorough testing will alone no longer be adequate to assure that the required system performance can be obtained. A deeper understanding will be required to make the effects of obscure design decisions clear at a level where their impact can be properly judged. This deeper understanding will be provided by tools and techniques that are just now being developed in research laboratories. Digital avionics systems will increasingly be the means by which many of the U.S. space goals will be accomplished. Now is an opportune time for the space vehicle community to step up to placing advanced, fault-tolerant avionic systems into general use by building on the experience of the aircraft industry supplemented by a fresh look at the tools and techniques for designing, fabricating and testing complex avionics systems.

Table 1
Organizations and Contacts

Organization	Contact
NASA Langley Research Center	Charles Meissner Felix Pitts
NASA Johnson Spaceflight Center	Tom Barry J. T. Edge
C. S. Draper Laboratory	Jay Lala John Deyst
Honeywell Systems Research Center	Mark Jeppson
Honeywell Commercial Flight Systems	Richard Hess Larry Yount
General Dynamics Space Systems	John Karas

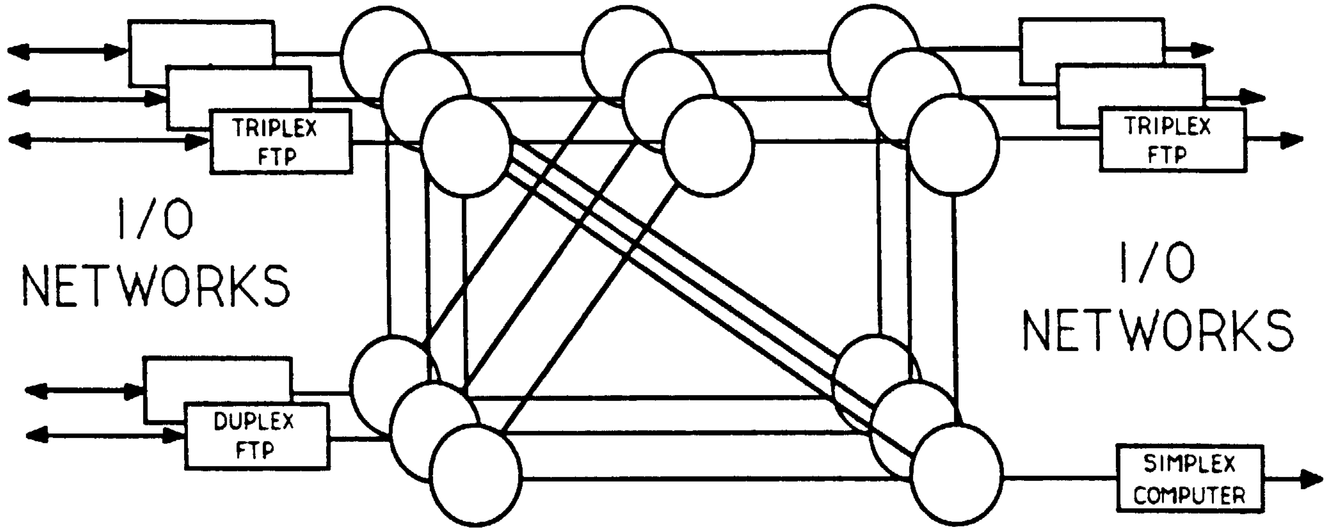
Table 1 (concluded)

Martin Marietta Astronautics Group	Robert Gates
Boeing Aerospace	Don Johnson
Lockheed/Sanders	Raymond Garbos
Wright Research and Dev. Center	Ron Szkody Raymond Bortner Jeff Stanley
Jet Propulsion Laboratory	David Rennels
Aerospace Corporation	George Gilley
Allied Signal ATC	Chris Walter
UCLA	Algirdas Avizienis
Fail Safe Technology	Mike Seavers

Table 2
conferences and Periodicals

Conference/Periodical	Sponsor
Digital Avionics System Conference	IEEE AIAA
Computers in Aerospace Conference	AIAA IEEE
Fault Tolerant Computing Symposium	IEEE
Reliability and Maintainability symposium	IEEE
National Aerospace Electronics Conference	IEEE
IEEE Transactions on Reliability	IEEE

Advanced Information Processing System



Features: **ADA Operating System**
Fault-Tolerant Distributed Processing Sites
Fault-Tolerant Inter-computer Network
Appropriate Function Reliability
Low Fault Tolerance Overhead
Growth Capability
Redundancy Transparent to User

Figure 1 - Advanced Information Processing System (AIPS)

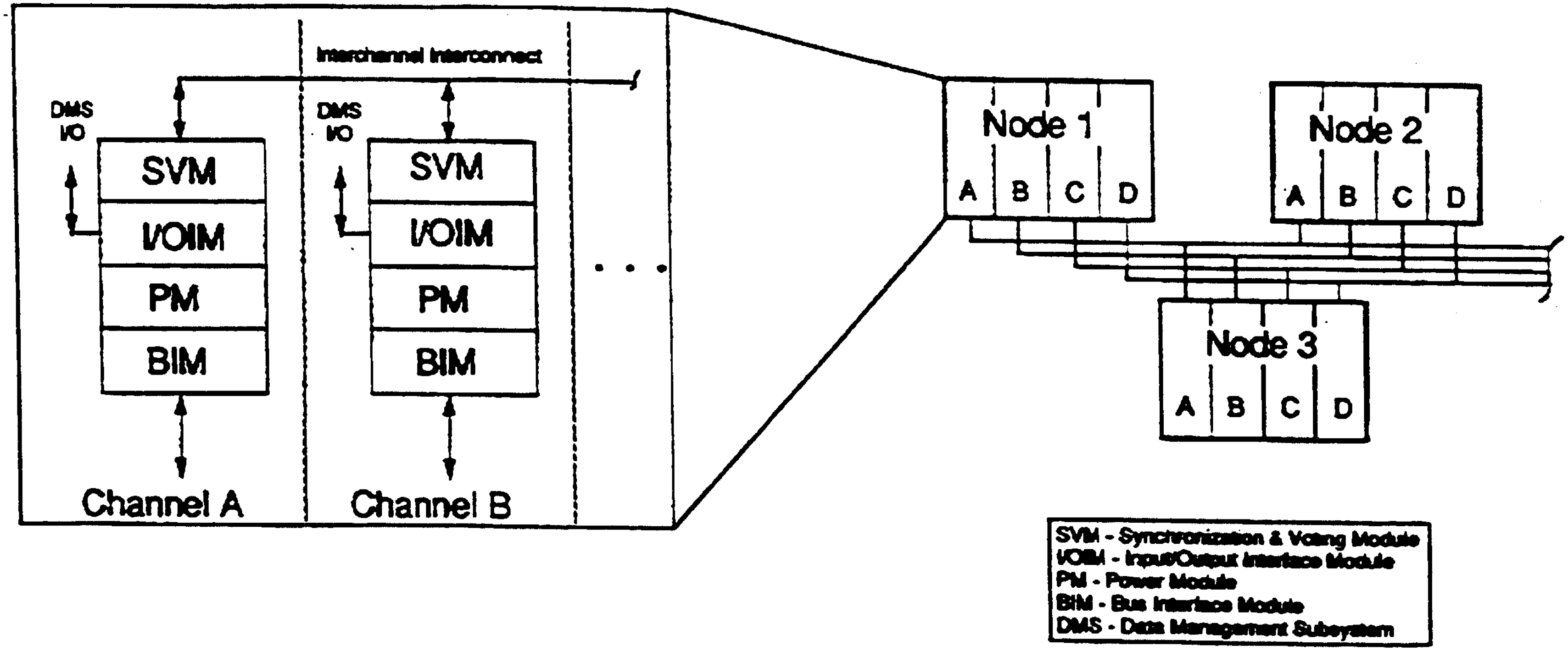

Interchannel Interconnect
DMS I/O
SVM
I/OIM
PM
BIM
Channel A
DMS I/O
SVM
I/OIM
PM
BIM
Channel B
Node 1
A B C D
Node 2
A B C D
Node 3
A B C D
SVM - Synchronization & Voting Module
I/OIM - Input/Output Interface Module
PM - Power Module
BIM - Bus Interface Module
DMS - Data Management Subsystem

Figure 2. IFTAS
Hybrid NMR Block Diagram

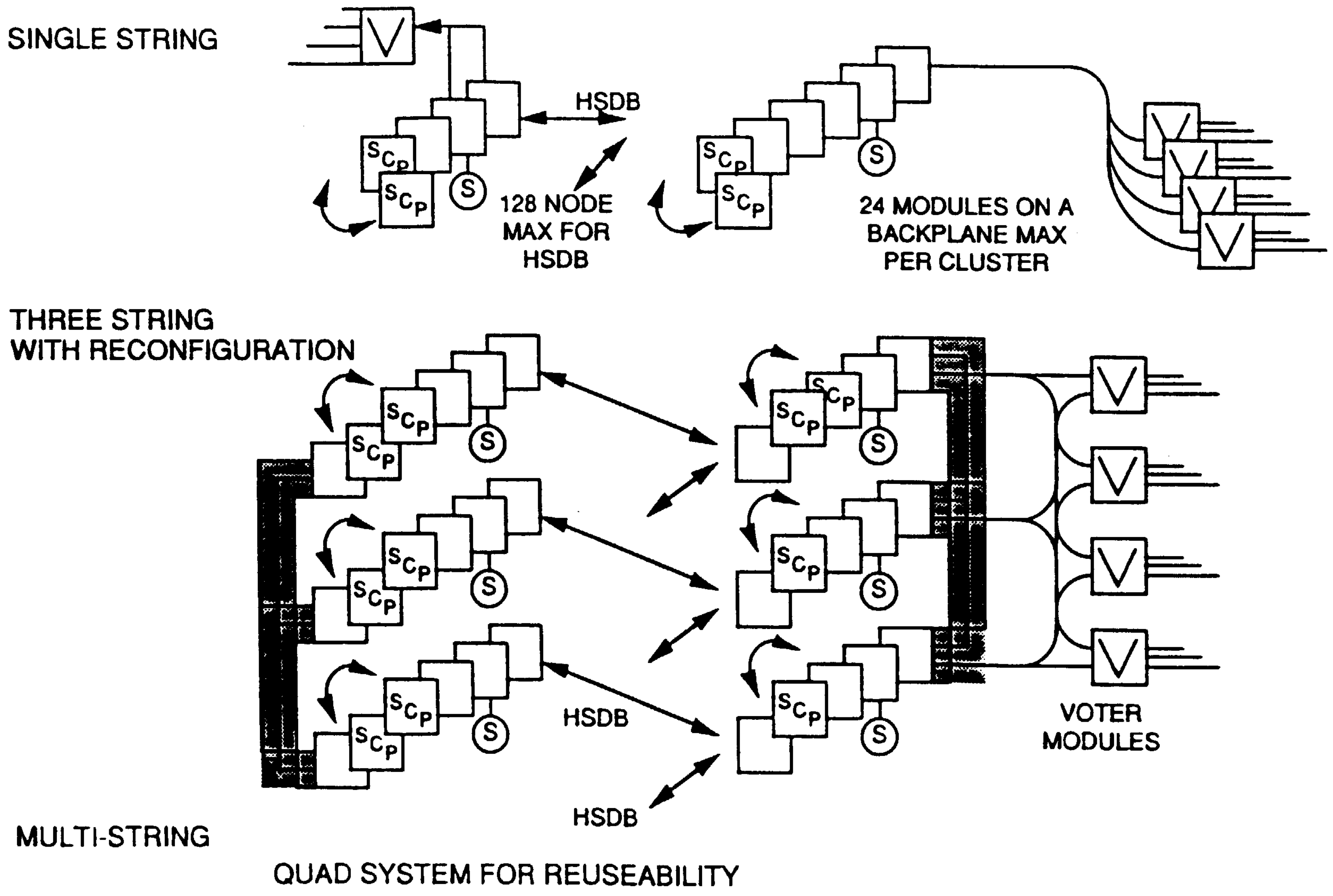

SINGLE STRING
HSDB
128 NODE MAX FOR HSDB
S_{C_P}
S_{C_P}
S
24 MODULES ON A BACKPLANE MAX PER CLUSTER
THREE STRING WITH RECONFIGURATION
HSDB
HSDB
VOTER MODULES
MULTI-STRING
QUAD SYSTEM FOR REUSEABILITY

Figure 3. MPRAS Architecture Configurations

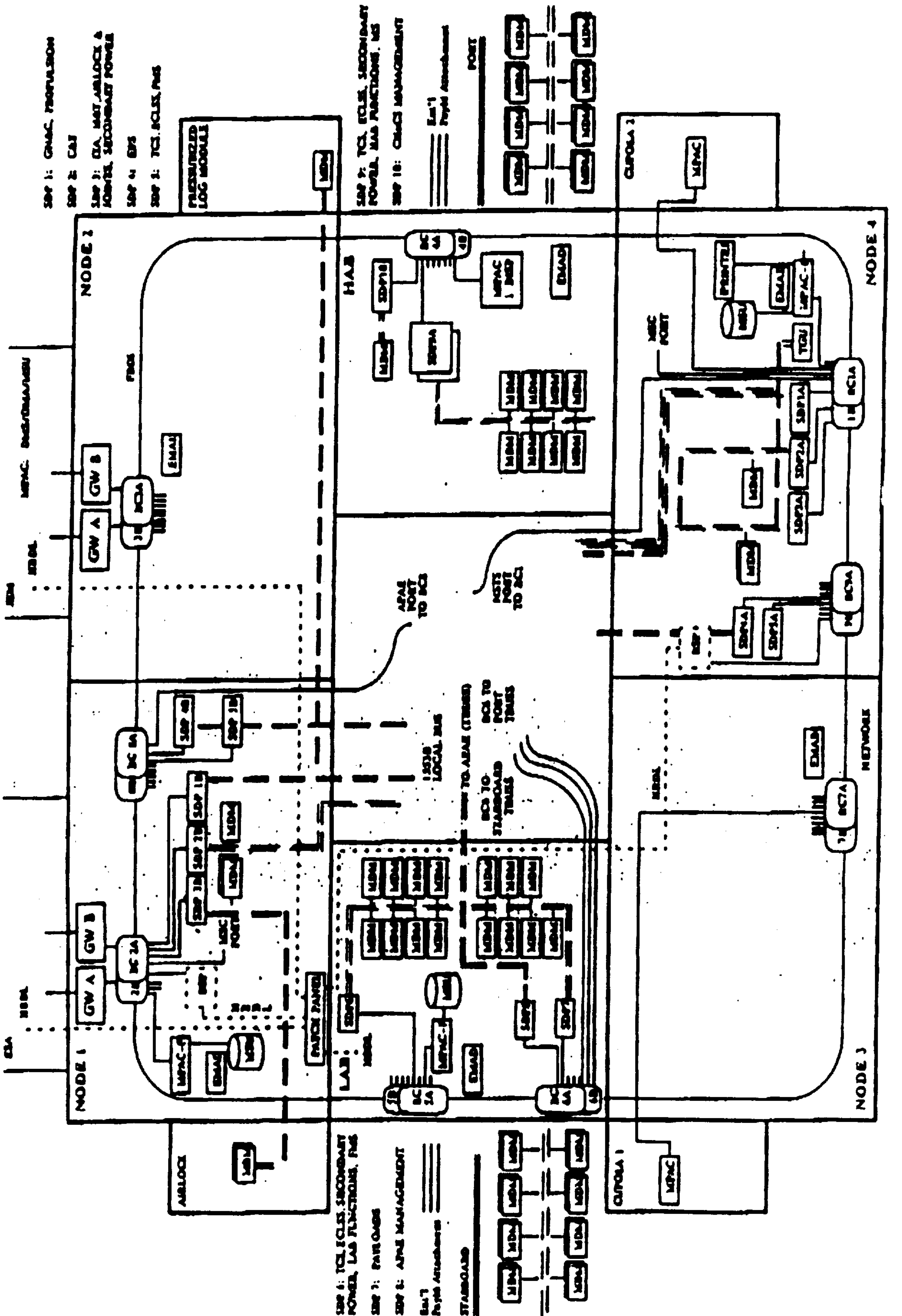
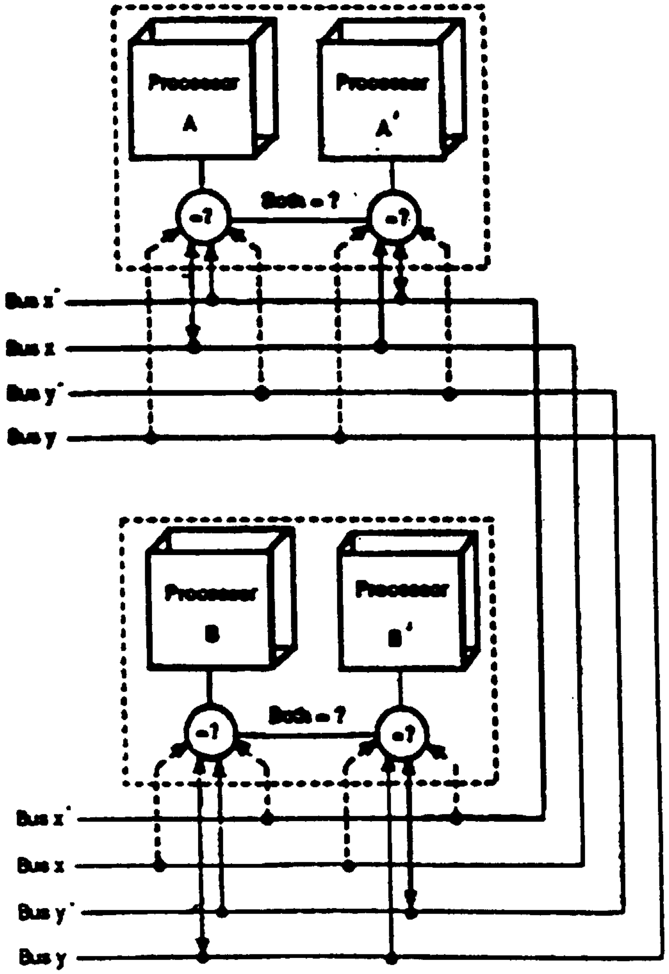


Figure 4. Space Station Freedom DMS Overview Schematic

ORIGINAL PAGE IS OF POOR QUALITY

Atomic Self-Checking Pairs

Honeywell



- **Characteristics**
  - Processors, Busses and Checkers are paired
  - Pairs are atomic (indivisible)
  - Each pair forms a fault containment zone
  - Halves of a pair are synchronous

- **Fault Detection**

  Near unity coverage, even the checkers are self-checking pairs

- **Fault Isolation**

  Unambiguous because of atomic property and has solution to the Byzantine Grenerals Problem

- **Fault Recovery**

  Fully distributed scheme means there is no mechanism that can become a single point of failure

KD>TBC/05/87/DS-9

Figure 5. Atomic Self-Checking Pairs